

86120



COPY OF PAPERS
ORIGINALLY FILED

212#6

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re U.S. Patent Application

Applicants: Yaakov Jordan Levy

Serial No.: 10/062,001

Filed: 02/01/2002

For: Improved OSS Signature Scheme

) I hereby certify that this correspondence is being deposited
) with the United Postal Service as first class mail in an
) envelope addressed to: Assistant Commissioner of Patents,
) Washington, DC 20231, on April 26, 2002

) 
) Gerald T. Shekleton Reg. No. 27,466 Date

RECEIVED
MAY 10 2002
Technology Center 2100

INFORMATION DISCLOSURE STATEMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Pursuant to 37 C.F.R. §1.97, a list of documents is disclosed on the attached Form PTO-1449 that may be material to the examination of this application. The cited references are enclosed herewith.

Documents for which the supplied date of publication lists the year of publication without the month were published sufficiently earlier than the effective U.S. filing date and any foreign priority date, so that the particular month of publication is not in issue. Pursuant to §609 of the MPEP, it is understood that the month of publication is not required when the particular month of publication is not in issue.

No inferences should be drawn that the attached list represents a comprehensive investigation, or that any material disclosed is equivalent to the subject invention. In addition, none of the documents that have publication dates prior to the priority date of the above application anticipate the invention in this application.

Applicant avers that no art cited herein was cited in a communication from a foreign Patent Office in a counterpart foreign application or, to the knowledge of the person signing the certification after making reasonable inquiry, was known to any individual designated in §1.56(c) more than three months prior to the filing of this Statement.

The cited document(s) disclose numerous specific features. There has been no attempt to list each and every feature disclosed by each document. The Examiner is requested to review the document(s) and determine the extent of the materiality of the document disclosures with respect to the present invention.

The discussion of any art and the citation of any document(s) herein is not to be construed as an admission that the art or document disclosure is necessarily within the invention field of endeavor, that the art or document disclosure is necessarily prior in time to a particular date which may be relevant to the instant patent application, and/or that the art or document disclosure is otherwise necessarily prior art as defined by the patent law with respect to the instant invention and application.

Also, there is reserved the right to later set forth how the instant invention is distinguished over the disclosure of any document or other art, including the disclosures of the art and document(s) recited herein, that may be cited by the Examiner in rejecting a claim in the instant patent application. The recitation herein of the art and document(s) is not to be construed as an assertion that more pertinent art could not possibly be in existence.

Respectfully submitted,

By Gerald T. Shekleton
Gerald T. Shekleton
Registration No. 27,466

Dated: April 26, 2002

WELSH & KATZ, LTD.

120 South Riverside Plaza
22nd Floor
Chicago, Illinois 60606
Telephone: 312-655-1500

**COPY OF PAPERS
ORIGINALLY FILED**

Sheet 1 of 1

(Rev. 5/92)
Comparable to
Form PTO-1449

U.S. Department of Commerce
Patent and Trademark Office

Atty. Docket No.

Serial No.

86120

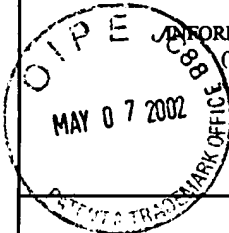
10/062,001

INFORMATION DISCLOSURE CITATION
(Use several sheets if necessary)

Applicants Yaakov (Jordan) Levy

Filing Date 02/01/2002

Group



U.S. PATENT DOCUMENTS

*Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date of Appropriate
	4,405,829	09/20/1983	RIVEST ET AL.			
	4,478,668	05/31/1988	SHAMIR ET AL.			

RECEIVED

MAY 10 2002

FOREIGN PATENT DOCUMENTS

Technology Center 2100

Document Number	Date	Country	Class	Subclass	Translation	
					Yes	No

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

	L. Adleman, D. Estes, and K. McCurley, "Solving Bivariate Quadratic Congruences in Random Polynomial Time," <i>Mathematics of Computation</i> , v. 48, n. 177, Jan 1987, pp. 17-28.
	D. Estes, L. Adleman, K. Kompella, K. McCurley, and G. Miller, "Breaking the Ong-Schnorr-Shamir Signature Scheme for Quadratic Number Fields," <i>Advances in Cryptology: Proceedings of CRYPTO '85</i> , Springer-Verlag, 1986, pp. 3-13
	Fiat and A. Shamir, "How to Prove Yourself: Practical Solutions to Identification and Signature Problems," <i>Advances in Cryptology: Proceedings of CRYPTO '86</i> , Springer-Verlag, 1987, pp. 186-194.
	D. Naccache, "Can O.S.S. be Repaired? Proposal for a New Practical Signature Scheme," <i>Advances in Cryptology: Proceedings of EUROCRYPT '93</i> , Springer-Verlag, 1994, pp. 233-239.
	National Institute of Standards and Technology, NIST FIPS PUB 186, "Digital Signature Standard," U.S. Department of Commerce, May 1994.
	H. Ong, C.P. Schnorr, and A. Shamir, "An Efficient Signature Scheme Based on Quadratic Equations," <i>Proceedings of the 16th Annual Symposium on the Theory of Computing</i> , 1984, pp. 208-216.
	H. Ong, C.P. Schnorr, and A. Shamir, "Efficient Signature Schemes Based on Polynomial Equations," <i>Advances in Cryptology: Proceedings of CRYPTO '84</i> , Springer-Verlag, 1985, pp. 37-46.
	J. Pollard and C. Schnorr, "An Efficient Solution of the Congruence $X^2 + k.y^2 = m \pmod{n}$," <i>IEEE Transactions on Information Theory</i> , v. IT-33, n. 5, Sep 1987, pp. 702-709.
	M. O. Rabin, "Digital Signatures and Public-Key Functions as Intractable as Factorization," MIT Laboratory for Computer Science, Technical Report, MLT/LCSFTR-212, Jan 1979.
	R. L. Rivest, A. Shamir, and L. M. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," <i>Communications of the ACM</i> , v. 21, n. 2, Feb 1978, pp. 120-126.

Examiner

Date Considered

*Examiner:

Initial if citation considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.